

Twisted Centralizer Codes

Adel Alahmadi*

S. P. Glasby^{†‡}

Cheryl E. Praeger^{†*}

Patrick Solé[§]

Bahattin Yildiz[¶]

March 14, 2017

Abstract

Given an $n \times n$ matrix A over a field F and a scalar $a \in F$, we consider the linear codes $C(A, a) := \{B \in F^{n \times n} \mid AB = aBA\}$ of length n^2 . We call $C(A, a)$ a *twisted centralizer code*. We investigate properties of these codes including their dimensions, minimum distances, parity-check matrices, syndromes, and automorphism groups. The minimal distance of a centralizer code (when $a = 1$) is at most n , however for $a \neq 0, 1$ the minimal distance can be much larger, as large as n^2 .

1 Introduction

Denote the $n \times n$ matrices over a field F by $F^{n \times n}$. Fix a matrix $A \in F^{n \times n}$ and a scalar $a \in F$. As we are motivated by applications to coding theory we focus on the case where F is a finite field \mathbb{F}_q of order q . The *centralizer of A , twisted by a* , is defined to be

$$(1) \quad C(A, a) := \{B \in F^{n \times n} \mid AB = aBA\}.$$

*Mathematics Department, King Abdulaziz University, Jeddah, Saudi Arabia.

[†]Center for Mathematics of Symmetry and Computation, University of Western Australia, 35 Stirling Highway, WA 6009, Australia. Email: Stephen.Glasby@uwa.edu.au, Cheryl.Praeger@uwa.edu.au

[‡]The Department of Mathematics, University of Canberra, ACT 2601, Australia.

[§]CNRS/LAGA, University of Paris 8, 2 rue de la Liberté, 93 526 Saint-Denis, France. Email: sole@enst.fr

[¶]University of Chester, UK. Email: bahattinyildiz@gmail.com

Key words: linear codes, matrix codes, minimal distance, group centralizers

MSC 2000 Classification: Primary 94B05, Secondary 13M05

Clearly $C(A, a)$ is an F -linear subspace of the vector space $F^{n \times n}$. Note that $C(A, 0)$ is the right-annihilator of A . We shall use the notation $C(A)$ instead of $C(A, 1)$ when $a = 1$, and note that $C(A)$ is simply the centralizer of A . The subspace $C(A, a)$ of $F^{n \times n}$ is viewed as code: we view a codeword $B \in F^{n \times n}$ as column vector $[B]$ of length n^2 , by reading the matrix B column-by-column. The case $a = 1$ was considered in [1]. In the present paper, we extend and sometimes correct the results of [1]. In particular the incorrect [1, Theorem 2.4] is corrected and generalized for this larger class of codes in [2] (see Theorem 2.3), and we exploit this result in several ways in Section 2.2.

Definition 1. For any $n \times n$ matrix $A \in F^{n \times n}$ and any scalar $a \in F$, the subspace $C(A, a)$ formed above is called the *centralizer code* obtained from A and *twisted by a* .

In a sense A serves as a parity-check matrix, because B lies in $C(A, a)$ precisely when $AB - aBA = 0$. More concretely, in the following result we show that a certain $n^2 \times n^2$ matrix H related to A is a parity check matrix in the sense that $B \in C(A, a)$ if and only if $H[B] = 0$, where $[B]$ is the n^2 -dimensional column vector above corresponding to B .

Proposition 1.1. *A parity-check matrix for $C(A, a)$ is given by*

$$H = I_n \otimes A - a(A^t \otimes I_n),$$

where \otimes denotes the Kronecker product, and A^t the transpose of the matrix A .

Proof. This follows from the proof of [10, Theorem 27.5.1, p.124] with $A = A$, $B = aA$, $C = 0$. Also, a direct proof (for row vectors) is given in [2, Lemma 3.2]. \square

The following simple observations involving $C(A, a)$ will be used later.

Theorem 1.2. *Suppose $a, a' \in F$ and $A \in F^{n \times n}$ is a matrix. Then the following are true:*

- a) $A \in C(A, a)$ if and only if $a = 1$ or $A^2 = 0$.
- b) If $B \in C(A, a)$ and $B' \in C(A, a')$ then BB' and $B'B$ both lie in $C(A, aa')$.
- c) For $a \neq 0$, $B \in C(A, a) \Leftrightarrow A \in C(B, a^{-1})$.
- d) For $A \neq 0_{n \times n}$, we have $I_n \in C(A, a) \Leftrightarrow a = 1$.
- e) For $a \neq 0$, $B \in C(A, a) \Leftrightarrow B^t \in C(A^t, a^{-1})$.

Proof. We only prove (b) since the other parts are simple observations. Starting from $AB = aBA$ and $AB' = a'B'A$, successive substitutions give

$$A(BB') = (AB)B' = aBAB' = aa'(BB')A.$$

\square

The problems about $C(A, a)$ that arise naturally for given A and a include:

- computing its dimension (k);
- deriving decoding/encoding algorithms and bounding the minimum distance (d);
- determining its automorphism group.

The paper is organized as follows. Sections 2, 3, 4 successively tackle the above three problems. Section 5 is dedicated to concrete examples of codes and Section 6 contains some concluding remarks and open problems. We say that $C(A, a)$ has *parameters* $[n^2, k, d]$ where $A \in F^{n \times n}$, $k = \dim(C(A, a))$, and d is the minimal (Hamming) weight of a nonzero vector. Note that $I_n \in C(A, 1)$, so the minimal distance of a centralizer code is at most n .

2 Dimension

2.1 Basic Bounds

Proposition 2.1. *If $A \in F^{n \times n}$, $a \in F$, and $C(A, a)$ contains an invertible matrix, then*

$$\dim C(A, a) = \dim C(A).$$

Proof. The result is true for $A = 0$ as $C(0, a) = F^{n \times n} = C(0)$. Suppose now that $A \neq 0$ and that $B \in C(A, a)$ is invertible. Then $B \in C(A, a)$ implies that $A = aBAB^{-1}$, and since $A \neq 0$ we must have $a \neq 0$. The linear map $\phi_B: C(A) \rightarrow C(A, a)$ with $X^{\phi_B} = XB$ is injective so $\dim C(A) \leq \dim C(A, a)$. Then $B^{-1} \in C(A, a^{-1})$ and $YB^{-1} \in C(A)$ for all $Y \in C(A, a)$. Hence the map $\psi_B: C(A, a) \rightarrow C(A)$ with $Y^{\psi_B} = YB^{-1}$ is the inverse of ϕ_B above. Therefore ψ_B is an isomorphism and $\dim C(A, a) = \dim C(A)$ as claimed. \square

The next result shows that for every n , with mild assumptions on A and a , the dimension of $C(A, a)$ is bounded above.

Proposition 2.2. *If $0 \neq A \in F^{n \times n}$ and $a \neq 1$, then $\dim(C(A, a)) \leq n^2 - 1$.*

Proof. If $\dim(C(A, a)) = n^2$, then every matrix B satisfies the relation $AB = aBA$. However if $B = I$ then $A = aA$ which does not hold. \square

In fact this bound can be improved to $\dim(C(A, a)) \leq n^2 - n$, see [2, Corollary 6.7].

2.2 Spectral bounds on the dimension of $C(A, a)$

In this section we treat matrices over the finite field \mathbb{F}_q . Some spectral notation is in order. For $B \in \mathbb{F}_q^{n \times n}$, let F denote a splitting field for the characteristic polynomial of B , and denote by $S(B) \subseteq F$ the set of its eigenvalues in F . Let $K(B, \lambda)$ denote the dimension over

F of the eigenspace (in F^n) corresponding to $\lambda \in S(B)$. Denote by $M(B, \lambda)$ the multiplicity of λ as a root of the characteristic polynomial of B . From linear algebra we know that $K(B, \lambda) \leq M(B, \lambda)$.

Theorem 2.3. [2, Theorem 4.7] *Let $a \in \mathbb{F}_q$ and $A \in \mathbb{F}_q^{n \times n}$. Then*

$$\sum_{\mu \in S(A)} K(A, a\mu)K(A^t, \mu) \leq \dim_{\mathbb{F}_q}(C(A, a)) \leq \sum_{\mu \in S(A)} M(A, a\mu)M(A^t, \mu).$$

An important consequence of the lower bound is the following, where $\text{Ker}(A)$ denotes the null space of A .

Corollary 2.4.

$$\dim C(A, a) \geq (\dim \text{Ker}(A))^2.$$

Proof. In the formula in Theorem 2.3, we may bound the sum below by the term indexed by $\mu = 0$. Note that $\dim \text{Ker}(A) = \dim \text{Ker}(A^t)$. Alternatively we may invoke Theorem 3.3 below. \square

The next Corollary explains why many matrices A yield codes $C(A, a) = \{0\}$.

Corollary 2.5. *If there is no $\lambda \in S(A)$ such that $\lambda a \in S(A)$ then $\dim(C(A, a)) = 0$.*

Proof. In the upper bound in Theorem 2.3, all the summands are zero. \square

The bounds are most useful when A is a combinatorial matrix with a known spectrum. Recall that an Hadamard matrix of order n is a $\{\pm 1\}$ valued matrix H satisfying $HH^t = nI$, see [9, 12]. The Kronecker product H_{2^k} of k copies of $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ are examples of degree 2^k .

Proposition 2.6. *Suppose $A \in \mathbb{F}_q^{n \times n}$ where q is a power of an odd prime p , and $p \nmid n$. If A is a symmetric Hadamard matrix with trace zero, then $\dim(C(A, a))$ equals $\frac{n^2}{2}$ if $a = \pm 1$, and 0 otherwise.*

Proof. Note that $p = \text{char}(\mathbb{F}_q) \nmid n$. By definition, $AA^t = nI$, and by hypothesis $A = A^t$, so that $A^2 = nI$. Thus the eigenvalues of A are $\pm\lambda$ where $\lambda^2 = n \neq 0$ in \mathbb{F}_q . Hence λ lies in $\mathbb{F}_{q^2}^\times$, and the Jordan form of A must be $\lambda I_k \oplus (-\lambda)I_{n-k}$ for some k with $0 < k < n$. However, $0 = \text{Trace}(A) = k\lambda + (n-k)(-\lambda)$ implies $k = n/2$. It follows that $K(A, \pm\lambda) = M(A, \pm\lambda) = n/2$. Thus if $a = \pm 1$ the upper and lower bounds of Theorem 2.3 coincide, and $\dim(C(A, a)) = 2(n/2)^2 = n^2/2$. If $a \neq \pm 1$, then $\dim(C(A, a)) = 0$ by Corollary 2.5. \square

Example 1: Let F be one of the fields \mathbb{F}_3 or \mathbb{F}_5 . Then, taking a Sylvester-type Hadamard matrix H_4 of order $n = 4$ yields an isodual* code $C(H_4, -1)$ over F with parameters $[16, 8, 4]$. The next order, that is, $H_4 \oplus H_4$ gives a $[64, 32, 8]$ code. Note that 8 is not a quadratic residue modulo 3 or modulo 5.

*An *isodual* code is one that is monomially equivalent to its dual.

3 Encoding-Decoding

Our approach to encoding-decoding procedures is similar to the case of ordinary centralizer codes $C(A)$ discussed in [1]. The codes $C(A, a)$ retain the advantage of efficient syndrome computation of the ordinary centralizer codes. An important difference is the much higher error correction capability of twisted codes with respect to the highly restricted capacity of the centralizer codes $C(A)$. If $C(A, a)$ has dimension k , then the *information rate* is k/n^2 , and we can give a procedure for encoding and decoding. As an \mathbb{F}_q -vector space, $C(A, a)$ has a basis consisting of k matrices, which we denote by $\{A_1, A_2, \dots, A_k\}$. We encode a given information vector (or message) $(a_1, a_2, \dots, a_k) \in \mathbb{F}_q^k$ as a codeword in $C(A, a)$, namely

$$a_1 A_1 + a_2 A_2 + \dots + a_k A_k.$$

The decoding can be done by reversing the above procedure. So, to find the message that a matrix $B \in C(A, a)$ represents, all we need is to find the coordinate vector for B in the basis $\{A_1, A_2, \dots, A_k\}$ of $C(A, a)$.

Note that $C(A, a)$ is an additive subgroup of $\mathbb{F}_q^{n \times n}$, and hence partitions $\mathbb{F}_q^{n \times n}$ into its additive cosets. Since a matrix $B \in \mathbb{F}_q^{n \times n}$ lies in $C(A, a)$ if and only if $AB - aBA = 0$, we can use A itself (instead of the $n^2 \times n^2$ matrix H in Proposition 1.1) as a type of parity-check matrix to obtain ‘syndromes’ which are determined by the cosets of $C(A, a)$. Thus we make the following definition:

Definition 2. Let $B \in \mathbb{F}_q^{n \times n}$ be any matrix over \mathbb{F}_q . The *syndrome* of B in $C(A, a)$ is defined as

$$\text{Synd}_{A,a}(B) = AB - aBA.$$

Thus $\text{Synd}_{A,a}$ is an F -linear map $F^{n \times n} \rightarrow F^{n \times n}$ and $B \in C(A, a) \Leftrightarrow \text{Synd}_{A,a}(B) = 0$. The following theorem suggests that this definition of the syndrome might help us in an error-correction scheme.

Theorem 3.1. Let $B_1, B_2 \in \mathbb{F}_q^{n \times n}$. Then $\text{Synd}_{A,a}(B_1) = \text{Synd}_{A,a}(B_2)$ if and only if B_1 and B_2 are in the same additive coset of $C(A, a)$.

Proof. The proof is similar to the proof of [1, Theorem 3.1] and is therefore omitted. \square

Testing whether a matrix B lies in $C(A, a)$ is the same as checking whether $\text{Synd}(B) = 0$. (We henceforth drop the subscripts on Synd .) Multiplying two $n \times n$ matrices has computational complexity of $O(n^m)$ field operations where $m \leq 2.373$, see the survey in [13]. Thus testing whether B lies in $C(A, a)$ using syndromes has the same complexity. Alternatively, one could use the $n^2 \times n^2$ parity check matrix H of Proposition 1.1. Since multiplying a vector in $\mathbb{F}_q^{n^2}$ by H (via the naïve algorithm) requires $O(n^4)$ field operations, the syndrome method is computationally advantageous.

We show in Subsection 3.1 that twisted centralizer codes have higher minimum distances, and hence higher error correction capability, than centralizer codes.

3.1 Bounds on the minimum distance

The distance d of a nonzero linear code is the minimal Hamming weight (number of nonzero coordinates) of a nonzero vector in the code. Thus the distance of $C(A, a)$ is at most n^2 .

Let J_n denote the $n \times n$ matrix with all entries equal to 1. The following theorem shows that there exist codes $C(A, a)$ whose minimal distance d is n^2 , which is as large as possible.

Theorem 3.2. *Suppose $J_n + I_n \in F^{n \times n}$ where $\text{char}(F)$ divides $n + 1$. If $a \neq 0, 1$, then the twisted centralizer code $C(J_n + I_n, a)$ equals $\langle J_n \rangle$ and has parameters $[n^2, 1, n^2]$.*

Proof. Let $A = J_n + I_n$, and let $p = \text{char}(F) > 0$. It follows from $J_n^2 = nJ_n$ that $J_n^p = n^{p-1}J_n = (-1)^{p-1}J_n = J_n$. Hence $A^p = (J_n + I_n)^p = J_n^p + I_n^p = A$. Let $u \in F^n$ be the column vector with all entries 1. Since $J_n u = nu$ and $Au = (n + 1)u = 0$, we see that $\det(A) = 0$. The null space of J_n has dimension $n - 1$, and so the same is true of the 1-eigenspace of A . Thus the Jordan form of A is the diagonal matrix $D = \text{diag}(0, 1, \dots, 1)$. A direct calculation using the fact that $a \neq 0, 1$ shows that $C(D, a) = \langle E_{11} \rangle$ is 1-dimensional. Since A and D are conjugate, the same is true for $\dim C(A, a)$. However, $J_n A = A J_n = (n + 1)J_n = 0$ and hence $C(A, a) = \langle J_n \rangle$. Therefore each nonzero element of $C(A, a)$ is bJ_n for some nonzero b , and hence $C(A, a)$ has minimum distance n^2 . In summary, $C(A, a)$ has parameters $[n^2, 1, n^2]$ as claimed. \square

A code with parameters $[N, k, d]$ must have $k + d \leq N + 1$. Hence if $N = d = n^2$, we conclude that $k = 1$ as happens in Theorem 3.2.

Experimental evidence using the programs [5] suggests that for any field other than \mathbb{F}_2 , and for any scalar other than 0 or 1, there exists some matrix $A \in F^{n \times n}$ such that $C(A, a)$ has parameters $[n^2, 1, n^2]$. Proving this claim for all $n \geq 2$ appears to be difficult without first guessing the *form* of suitable matrices A , and even then the computations can depend in a complicated way on the field F . Let $A_n = E_{n,1} - E_{n,n} + \sum_{i=1}^{n-1} E_{i,i} - E_{i,i+1}$, and let $B_n = J_n - 2 \sum_{i=1}^n E_{i,n}$. When $n = 4$ these matrices are

$$A_4 = \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 0 & 0 & -1 \end{pmatrix}, \quad \text{and} \quad B_4 = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

If the characteristic of F is zero, then a variant of the proof of Theorem 3.2 shows that $C(A_n, -1) = \langle B_n \rangle$. However, our focus is on *finite* fields, and here one can only prove this when $\text{char}(F)$ is ‘sufficiently large’. The idea is to solve the system $A_n X + X A_n = 0$ for $X \in \mathbb{Z}^{n \times n}$, thereby determining ‘bad’ primes which will increase the rank of the solution space. For example, $C(A_n, -1) = \langle B_n \rangle$ holds when $n = 3$ provided $\text{char}(F) \neq 2$, and when $n = 30$ provided $\text{char}(F)$ is not one of 27 ‘bad’ characteristics. The bad characteristics have $k = \dim C(A_n, -1) > 1$, and hence $d < n^2$. They have much larger information rates k/n^2 , but may correct fewer errors.

3.2 An upper bound

An \mathbb{F}_q -linear code C is said to have *parameters* $[N, K, d]$ if C is a K -dimensional subspace of \mathbb{F}_q^N (consisting of column vectors), d is the minimum distance of C , and N is called the *length* of C . Sometimes we omit d and say that C is an $[N, K]$ code over \mathbb{F}_q . If D, E are two F -linear codes of the same length N , we write their *product code* as

$$D \otimes E = \{uv^t \mid u \in D, v \in E\} \subseteq F^{N \times N}.$$

Theorem 3.3. *For all $a \in \mathbb{F}_q$, the code $C(A, a)$ contains the product code $\text{Ker}(A) \otimes \text{Ker}(A^t)$. If $\text{Ker}(A), \text{Ker}(A^t)$ have respective parameters $[n, k, d]$ and $[n, k', d']$, then $C(A, a)$ has parameters $[n^2, K, D]$ with $K \geq kk'$ and $D \leq dd'$.*

Proof. If $u \in \text{Ker}(A)$, and $v \in \text{Ker}(A^t)$, (both column vectors) then $B = uv^t \in C(A, a)$, since $AB = (Au)v^t = 0$, and $BA = u(A^t v)^t = 0$. The second statement follows by standard properties of product codes [9]. \square

This result leads to a general upper bound on the minimum distance $d(A, a)$ of $C(A, a)$. Denote by $\Delta_q(N, K)$ the largest minimum distance of all $[N, K]$ codes over \mathbb{F}_q .

Corollary 3.4. *For all $a \in \mathbb{F}_q$, and $A \in \mathbb{F}_q^{n \times n}$,*

$$d(A, a) \leq (\Delta_q(n, k_0))^2, \quad \text{where } k_0 = \dim_q(\text{Ker}(A)).$$

Proof. Both $\text{Ker}(A)$ and $\text{Ker}(A^t)$ have the same dimension k_0 . The result follows by the second statement of Theorem 3.3. \square

Theorem 3.3 also gives the following lower bound for the minimum distance $d(A, a)$ of $C(A, a)$ for rank 1 matrices A .

Corollary 3.5. *If A has rank one then $d(A, a)$ is at most 4.*

Proof. Since A has rank 1, both $\text{Ker}(A)$ and $\text{Ker}(A^t)$ have dimension $n - 1$. Hence either $\text{Ker}(A)$ contains a weight 1 vector, or two distinct weight 1 vectors not in $\text{Ker}(A)$ will differ by a weight 2 vector, which must lie in $\text{Ker}(A)$. Thus $\text{Ker}(A)$ contains a nonzero vector of weight at most 2, and hence (when regarded as a code in \mathbb{F}_q^n) it has minimum distance at most 2. The same is true for $\text{Ker}(A^t)$, and the result now follows from the second statement of Theorem 3.3. \square

3.3 A lower bound: asymptotics

Recall the q -ary entropy function defined for $0 < x < \frac{q-1}{q}$ by

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$

This quantity is instrumental in the estimation of the volume of high-dimensional Hamming balls when the base field is \mathbb{F}_q . The result we are using is that the volume of the Hamming ball of radius xn in \mathbb{F}_q^n is, up to subexponential terms, $q^{nH_q(x)}$, when $0 < x < 1$ and n goes to infinity [8, Lemma 2.10.3].

Theorem 3.6. *For $a \neq 0, 1$, and for $n \rightarrow \infty$, there are codes $C(A, a)$ with minimum distance at least $\frac{n}{\log n}$.*

Proof. Let $B \in \mathbb{F}_q^{n \times n}$ be nonzero and have weight less than $\frac{n}{\log n}$. Then $B \in C(A, a)$ if and only if $A \in C(B, a^{-1})$, by Theorem 1.2(c). Thus the number of codes $C(A, a)$ containing B is $|C(B, a^{-1})|$, and by [2, Prop. 6.6], this is at most $X := q^{n^2 - 2n + 2}$.

As we mentioned above, by [8, Lemma 2.10.3], the number of such matrices B is $q^{n^2 H_q(Y)}$ where $Yn^2 = \frac{n}{\log n}$, that is, $Y = \frac{1}{n \log n}$. Thus the total number of codes $C(A, a)$ which contain at least one nonzero matrix B of weight less than $\frac{n}{\log n}$ is at most $X q^{n^2 H_q(Y)} = q^{n^2 - 2n + 2 + n^2 H_q(Y)}$. The result will follow if we can show that this quantity is less than the total number of these codes $C(A, a)$ which are nonzero. By [2, Theorem 5.2], the total number of these nonzero codes is at least $\frac{1}{q} \times q^{n^2} = q^{n^2 - 1}$.

Now $H_q(x) = -x \log_q x + O(x)$, for small x (see, for example, [7, Proposition 3.3.6]), and hence for $n \rightarrow \infty$, we have

$$n^2 H_q(Y) = n^2 H_q\left(\frac{1}{n \log n}\right) \sim -\frac{n}{\log n} \log_q \frac{1}{n \log n} \sim \frac{n}{\log q}.$$

Thus $n \sim n^2 H_q(Y) \log q = \log(q^{n^2 H_q(Y)})$, and hence $q^{n^2 H_q(Y)} \sim q^n$.

Therefore, for large n , the number of codes $C(A, a)$ which contain at least one nonzero matrix B of weight less than $\frac{n}{\log n}$ is at most $q^{n^2 - 2n + 2 + n^2 H_q(Y)} \sim q^{n^2 - n + 2}$, which is less than $q^{n^2 - 1}$. We can now conclude that there exist codes in the family that have minimum distance at least $\frac{n}{\log n}$. \square

3.4 An example of error-correction for rank 1 matrices

We discuss the twisted centralizer codes $C(A, a)$ for the case where A is a rank 1 matrix in $\mathbb{F}_q^{n \times n}$. The dimensions of such codes were determined in [2, Remark 2.10], and all are of the form $(n - 1)^2 + \delta$. Indeed if $a \neq 0, 1$, then $\delta = 1$ when $A^n = 0$ and $\delta = 0$ otherwise. However the minimum distance $d(A, a)$, and hence the error-correcting properties, are not so uniformly described.

For example, if $A = E_{11}$, the matrix with entry 1 in the $(1, 1)$ -position and all other entries zero, then for any value of a , the code $C(E_{11}, a)$ is easy to compute, and in particular for each of the $(n - 1)^2$ pairs (i, j) with $i > 1$ and $j > 1$, $C(E_{11}, a)$ contains the weight 1 matrix E_{ij} (with a single nonzero entry, namely an entry 1 in the (i, j) -position). Thus $d(E_{11}, a) = 1$, which is unfortunately smaller than the upper bound given in Corollary 3.5.

We show in Theorem 3.7 that the upper bound of Corollary 3.5 is often achieved for a different family of rank 1 matrices, namely the matrices J_n where J_n has degree n and has all entries equal to 1. This illustrates, in particular, that conjugating $C(A, a)$ by an element of $\text{GL}(n, q)$ can change the minimal distance of the code.

The ‘single errors’ that may occur are the weight 1 matrices bE_{ij} , where $b \in \mathbb{F}_q \setminus \{0\}$. We say that a code $C(A, a)$ *corrects single errors* if distinct single errors B, B' give distinct syndromes $\text{Synd}(B)$ and $\text{Synd}(B')$. Our next result shows that the codes $C(J_n, a)$ can be used for single error correction.

Theorem 3.7. *Let $q \geq 3$, $n \geq 2$, and $a \in \mathbb{F}_q \setminus \{0, 1\}$. Then the code $C(J_n, a)$ corrects single errors. Moreover,*

- (a) *if either $n \geq 3$ or q is odd, then $d(J_n, a) = 4$ and, for example, $E_{11} - E_{12} - E_{21} + E_{22}$ is a minimum weight nonzero codeword; while*
- (b) *if $n = 2$ and q is even (so $q \geq 4$), then $d(J_n, a) = 3$ and $aE_{11} + (a - 1)E_{12} + E_{22}$ is a minimum weight nonzero codeword.*

Proof. As discussed above, a single error is a matrix bE_{ij} , with $b \neq 0$ and $1 \leq i, j \leq n$. A simple computation shows that the syndrome $\text{Synd}(bE_{ij}) = J_n(bE_{ij}) - a(bE_{ij})J_n = bS(i, j)$, where $S(i, j) = \text{Synd}(E_{ij})$ is the matrix with (k, ℓ) -entry described below

$$S(i, j)_{k\ell} = \begin{cases} 0 & \text{if } k \neq i \text{ and } \ell \neq j \\ 1 & \text{if } k \neq i \text{ and } \ell = j \\ -a & \text{if } k = i \text{ and } \ell \neq j \\ 1 - a & \text{if } k = i \text{ and } \ell = j. \end{cases}$$

In particular, since all of these syndromes are nonzero, it follows that $C(J_n, a)$ contains no weight one matrices, so $d(C(J_n, a)) \geq 2$.

Next we consider a weight two matrix $B = b_1E_{i_1j_1} + b_2E_{i_2j_2}$ with $(i_1, j_1) \neq (i_2, j_2)$, $i_1 \leq i_2$, $b_1 \neq 0$ and $b_2 \neq 0$. Then $S := \text{Synd}(B) = b_1S(i_1, j_1) + b_2S(i_2, j_2)$. Suppose first that $i_1 \neq i_2$ and $j_1 \neq j_2$. Up to row and column permutations, the $\{i_1, i_2\} \times \{j_1, j_2\}$ -submatrix of S is

$$(2) \quad \begin{pmatrix} b_1(1 - a) & b_2 - ab_1 \\ b_1 - ab_2 & b_2(1 - a) \end{pmatrix}.$$

Since $a \neq 1$ we see $b_1(1 - a) \neq 0$, so $S \neq 0$. Next suppose that $i_1 = i_2$, so that we must have $j_1 \neq j_2$ since B has weight two. For $i \neq i_1$, the entry $S_{i,j_1} = b_1 \neq 0$, so $S \neq 0$. A similar argument shows that $S \neq 0$ if $j_1 = j_2$. Thus $S \neq 0$ for all weight two matrices B , which implies that $d(C(J_n, a)) \geq 3$.

A straightforward computation shows that, if $B = E_{11} + E_{22} - E_{12} - E_{21}$, then $\text{Synd}(B) = 0$, and hence $B \in C(J_n, a)$. Thus it remains to consider whether $C(J_n, a)$ contains a weight

three codeword B . Suppose then that $B = b_1 E_{i_1 j_1} + b_2 E_{i_2 j_2} + b_3 E_{i_3 j_3}$ with distinct pairs (i_k, j_k) and nonzero b_k , for $k = 1, 2, 3$, and let $S := \text{Synd}(B) = \sum_{k=1}^3 b_k S(i_k, j_k)$. Suppose that $B \in C(J_n, a)$, or equivalently, that $S = 0$.

First assume that $i_1 \neq i_2$ and $j_1 \neq j_2$, and let $S' = \text{Synd}(b_1 E_{i_1 j_1} + b_2 E_{i_2 j_2})$. The $\{i_1, i_2\} \times \{j_1, j_2\}$ -submatrix of S' is as in (2). As each of the diagonal entries of this restriction is nonzero, and as $S = S' + b_3 S(i_3, j_3) = 0$, it follows that (i) either $i_3 = i_1$ or $j_3 = j_1$; and also (ii) either $i_3 = i_2$ or $j_3 = j_2$. Considering transposes if necessary, we may therefore assume that $i_3 = i_1$ and $j_3 = j_2$. If $n \geq 3$ then, for $i \notin \{i_1, i_2\}$, the entry $S_{ij_1} = b_1 \neq 0$, which is a contradiction. Thus $n = 2$, and

$$S = \begin{pmatrix} b_1(1-a) - b_3 a & b_2 - ab_1 + b_3(1-a) \\ b_1 - ab_2 & b_2(1-a) + b_3 \end{pmatrix} = 0.$$

It follows that $b_1 = b_2 a$ (from the (i_2, j_1) -entry), $b_3 = -b_2(1-a)$ (from the (i_2, j_2) -entry), and then from these equalities and the (i_1, j_1) -entry we find

$$0 = b_1(1-a) - b_3 a = 2b_2 a(1-a)$$

so that, since $b_2 a(1-a) \neq 0$, we must have q even. The (i_1, j_2) -entry is $2b_2 a(1-a)$ which is zero since q is even. Thus $B = b_2(aE_{i_1 j_1} + E_{i_2 j_2} + (1-a)E_{i_1 j_2})$ has zero syndrome and hence $d(J_2, a) = 3$ and part (b) holds. Finally we may assume that, for each pair $(k, \ell) = (1, 2), (2, 3)$ or $(3, 1)$, either $i_k = i_\ell$ or $j_k = j_\ell$. Without loss of generality, and transposing if necessary, we may assume that $i_1 = i_2$ (so $j_1 \neq j_2$, since B has weight three). Suppose that $i_3 \neq i_1$. Then we must have both $j_3 = j_1$ and $j_3 = j_2$, which is impossible. Hence also $i_3 = i_1$, and j_1, j_2, j_3 are pairwise distinct. However this implies that, for $i \neq i_1$, the entry $S_{ij_1} = b_1 \neq 0$. This contradiction completes the proof. \square

Proposition 3.8. *Suppose $J_n \in \mathbb{F}_q^{n \times n}$ where $n \geq 3$ or q is odd, and $a \in \mathbb{F}_q \setminus \{0, 1\}$. The parameters of $C(J_n, a)$ are $[n^2, (n-1)^2 + 1, 4]$ if $\text{char}(\mathbb{F}_q) \mid n$, and $[n^2, (n-1)^2, 4]$ otherwise.*

Proof. Since $n \geq 3$ or q is odd, the minimum distance is 4 by Theorem 3.7. However, $J_n^2 = nJ_n$ implies that J_n is nilpotent if and only if the characteristic p of \mathbb{F}_q divides n . Therefore by [2, Remark 2.10] the dimension of $C(J_n, a)$ is $(n-1)^2 + 1$ if $p \mid n$, and it is $(n-1)^2$ otherwise. \square

4 Automorphism group

If A and A' are conjugate under the general linear group $\text{GL}(n, F)$, then the codes $C(A, a)$ and $C(A', a)$ have the same dimension, but almost certainly different minimal distances. However, if A and A' are conjugate by a monomial matrix, then $C(A, a)$ and $C(A', a)$ do have the same minimal distances. The centralizer of A in $\text{GL}(n, F)$ induces automorphisms of $C(A, a)$.

The *adjacency matrix* of a graph Γ with vertex set $\{1, \dots, n\}$, is an $n \times n$ matrix with (i, j) -entry 1 or 0 according as vertex i and vertex j are, or are not, adjacent in Γ . Adjacency matrices can be interpreted as matrices over any field F .

Theorem 4.1. *If $A \in F^{n \times n}$ is the adjacency matrix of a graph Γ and $G = \text{Aut}(\Gamma)$, then the direct product $G \times G$ acts on the code $C(A, a)$ by coordinate permutations.*

Proof. As is well-known [3], a permutation matrix P lies in $\text{Aut}(\Gamma)$ if and only if $PA = AP$, that is if and only if $P \in C(A)$. Given $(P, Q) \in G \times G$ and $B \in C(A, a)$, it follows from Theorem 1.2 (b) that $P^{-1}BQ$ lies in $C(A, a)$. It is easy to verify that $B^{(P, Q)} = P^{-1}BQ$ defines an action of $G \times G$ on $C(A, a)$. This corresponds to the so called ‘product action’ of $G \times G$ permuting the n^2 coordinates of the codewords of $C(A, a)$ (read off column by column). \square

A *semiregular* permutation is a non-identity permutation, all cycles of which have the same length. For a positive integer n and a divisor ℓ of n , a code of length n is called *ℓ -quasicyclic* if a cyclic shift of each codeword by ℓ positions results in another codeword.

Corollary 4.2. *If $A \in F^{n \times n}$ is the adjacency matrix of a graph admitting a semiregular automorphism with m cycles, then $C(A, a)$ is up to equivalence (n^2/m) -quasicyclic.*

Proof. This follows from Theorem 4.1 on taking the semiregular automorphism to act either on the rows or the columns of the matrix codewords. \square

Corollary 4.3. *If $A \in F^{n \times n}$ is a permutation matrix corresponding to a cycle of length n , then $C(A, a)$ is equivalent to an n -quasicyclic code.*

Proof. Take $m = n$ in Corollary 4.2. \square

Consider the following elementary observation. We call the map $B \mapsto B^t$ the *transposition permutation*. This permutation on n^2 elements can act on the coordinate entries of $C(A, a)$ as the next result shows, *c.f.* Theorem 1.2(e).

Proposition 4.4. *If $B \in C(A, a)$ and $a \neq 0$, then $B^t \in C(A^t, a^{-1})$. In particular if $A^t = \pm A$, then $C(A, 1)$ and $C(A, -1)$ are invariant under the transposition permutation.*

Proof. Observe that $AB = aBA \Leftrightarrow A^t B^t = a^{-1} B^t A^t$, and $a = a^{-1} \Leftrightarrow a = \pm 1$. \square

5 Examples

Twisted centralizer codes give examples of many types of interesting codes, including *optimal* codes, see [8, §2.1], and codes with large minimal distance. Given $A \in F^{n \times n}$, the centralizer code $C(A, 1)$ has minimal distance at most n because $I_n \in C(A, 1)$. By contrast, when $a \neq 0, 1$, the twisted centralizer codes $C(A, a)$ can have larger distances as illustrated strikingly in Theorem 3.2. This section provides examples of codes $C(A, a)$ that are optimal and have $a \neq 0, 1$. The results below were computed using MAGMA [4] code [5] and using Proposition 1.1, where optimality was confirmed using [6].

5.1 (-1) -centralizer codes over \mathbb{F}_3

The codewords of $C(A, a)$ are easily described when $a = 0, 1$, see for example [11] for $a = 1$. In this subsection we consider twisted centralizer codes over \mathbb{F}_3 or \mathbb{F}_5 with $a = -1$.

Case 1: $n = 3$. For each $A \in \mathbb{F}_3^{3 \times 3}$ we compute the parameters $[N, k, d]$ for the twisted centralizer codes $C(A, -1)$. Since $N = n^2 = 9$ we list the possible pairs $[k, d]$ with the multiplicity as a superscript. The sum of the multiplicities is $|\mathbb{F}_3^{3 \times 3}| = 3^9$.

$$\begin{aligned} &[0, *]^{7722}, [1, 1]^{90}, [1, 2]^{720}, [1, 3]^{720}, [1, 4]^{900}, [1, 6]^{720}, [1, 9]^{360}, [2, 1]^{624}, [2, 2]^{1140}, [2, 3]^{480}, \\ &[2, 4]^{1272}, [2, 5]^{384}, [2, 6]^{1248}, [3, 1]^{414}, [3, 2]^{876}, [3, 3]^{416}, [3, 4]^{840}, [3, 5]^{144}, [3, 6]^{40}, \\ &[4, 1]^{216}, [4, 2]^{204}, [4, 4]^{48}, [5, 1]^{48}, [5, 2]^{48}, [5, 4]^8, [9, 1]^1. \end{aligned}$$

The entry $[9, 1]^1$ means that only $A = 0$ has $C(A, -1) = \mathbb{F}_3^{3 \times 3}$, and $[0, *]^{7722}$ means that 7722 matrices $A \in \mathbb{F}_3^{3 \times 3}$ have $C(A, -1) = \{0\}$. By convention, the minimal distance of the zero subspace of $F^{n \times n}$ is $d = n^2$. The above data were computed using the computer code [5].

Remark 1. The ternary codes with parameters $[9, 5, 4]$, $[9, 3, 6]$, $[9, 2, 6]$, $[9, 1, 9]$ are all optimal ternary codes according to [6]. This contrasts with ordinary centralizer codes, where the minimum distances are at most n (and here $n = 3$).

Case 2: $n = 4$. Suppose $A \in \mathbb{F}_3^{4 \times 4}$. The codes $C(A_i, -1)$ where A_i is listed below are optimal ternary codes

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 2 & 1 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 2 & 0 & 1 & 2 \\ 2 & 1 & 2 & 0 \\ 1 & 1 & 0 & 2 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 2 & 1 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 1 & 2 & 1 & 1 \end{pmatrix},$$

with parameters $[16, 2, 12]$, $[16, 3, 10]$, $[16, 4, 9]$ and $[16, 10, 4]$, respectively.

Remark 2. Given a 4×4 matrix A , the centralizer code $C(A)$ (with $a = 1$) can correct at most 1 error since $d(C(A)) \leq 4$. By contrast, $C(A_1, -1)$ above can correct 5 errors and the two codes have the same information rates when $\dim C(A) = 2$.

5.2 2-centralizer codes over \mathbb{F}_5

We give examples of optimal \mathbb{F}_5 -linear codes of the form $C(A, 2)$.

Case 1: $n = 2$. If $A = \begin{pmatrix} 1 & 1 \\ 4 & 4 \end{pmatrix} \in \mathbb{F}_5^{2 \times 2}$, then $C(A, 2)$ is an \mathbb{F}_5 -linear code with parameters $[4, 2, 3]$. Note that this code is also an MDS-code. Recall that it is impossible to have a

one-error correcting code from the centralizer of a 2×2 matrix, but we are able to do so with the 2-twist.

Case 2: $n = 3$. The matrices $A_1, A_2, A_3 \in \mathbb{F}_5^{3 \times 3}$ below

$$A_1 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 2 & 0 & 3 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 3 & 3 & 3 \end{pmatrix},$$

give optimal codes $C(A_1, 2), C(A_2, 2), C(A_3, 2)$ with parameters $[9, 2, 7], [9, 3, 6]$ and $[9, 5, 4]$, respectively.

Case 3: $n = 4$. The matrices $A_1, A_2 \in \mathbb{F}_5^{4 \times 4}$ below

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 4 & 0 \\ 3 & 2 & 2 & 2 \\ 4 & 3 & 4 & 4 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 4 & 0 \\ 3 & 2 & 2 & 4 \\ 3 & 3 & 1 & 2 \end{pmatrix},$$

give optimal codes $C(A_1, 2), C(A_2, 2)$ with parameters $[16, 2, 13], [16, 3, 12]$, respectively.

6 Conclusion

In this paper, we have introduced and studied twisted centralizer codes, a non-trivial generalization of the centralizer codes of [1]. The incorrect dimension formula of [1, Theorem 2.4] was replaced by lower and upper bounds on the dimension of $C(A, a)$ in [2, Theorem 4.7] (Theorem 2.3). The lower bound is especially relevant when the spectrum of A contains eigenvalues in the ratio of a . These bounds were exploited in Section 2 to obtain explicit results for examples from Hadamard matrices. It would be worthwhile to find more examples based on combinatorial matrices (adjacency matrices of graphs and designs). The absolute upper bound on the dimension of $C(A, 1)$ [1, Theorem 2.1] as a function of n is not easy to generalize to $a \neq 1$. The proof of the Kronecker product expression for the parity-check matrix has been simplified. An upper bound on the minimum distance based on the concept of product codes has been derived.

Our computational evidence indicates that twisted centralizer codes can have much higher minimal distances than centralizer codes. Thus they retain the computational advantages of centralizer codes while having much higher error-correction capacity. The error-correction itself can sometimes be more simply expressed as was demonstrated by the example of J_n in Section 3.4.

Acknowledgement: We would like to thank the referee for making helpful suggestions. The fourth author thanks Prof. Rioul for helpful discussions.

References

- [1] Adel Alahmadi, Shefa Alamoudi, Suat Karadeniz, Bahattin Yildiz, Cheryl E. Praeger, and Patrick Solé, *Centraliser codes*, Linear Algebra Appl. **463** (2014), 68–77, DOI 10.1016/j.laa.2014.08.024. MR3262389 ↑2, 5, 13, 14
- [2] Adel Alahmadi, S.P. Glasby, and Cheryl E. Praeger, *On the dimension of twisted centralizer codes*, arXiv:1607.05838 (2016). ↑2, 3, 4, 8, 10, 13
- [3] Norman Biggs, *Algebraic graph theory*, 2nd ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1993. MR1271140 ↑11
- [4] Wieb Bosma, John Cannon, and Catherine Playoust, *The MAGMA algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsc.1996.0125. Computational algebra and number theory (London, 1993). MR1484478 ↑12
- [5] S.P. Glasby, *Programs in MAGMA for calculating minimal distances* (2016). Online available at www.maths.uwa.edu.au/~glasby/. ↑6, 12
- [6] Markus Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Online available at www.codetables.de. ↑12
- [7] V. Guruswami, A. Rudra, and M. Sudan, *Essential coding theory* (2015). Online available at www.cse.buffalo.edu/faculty/atri/courses/coding-theory/book/. ↑8
- [8] W. Cary Huffman and Vera Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, Cambridge, 2003. MR1996953 ↑8, 12
- [9] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes, I and II*, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977. North-Holland Mathematical Library, Vol. 16. MR0465510 ↑4, 7
- [10] V. V. Prasolov, *Problems and theorems in linear algebra*, Translations of Mathematical Monographs, vol. 134, American Mathematical Society, Providence, RI, 1994. Translated from the Russian manuscript by D. A. Leites. MR1277174 ↑2
- [11] Richard Stong, *Some asymptotic results on finite vector spaces*, Adv. in Appl. Math. **9** (1988), no. 2, 167–199, DOI 10.1016/0196-8858(88)90012-7. MR937520 ↑12
- [12] W. D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis, *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Lecture Notes in Mathematics, Vol. 292, Springer-Verlag, Berlin-New York, 1972. MR0392580 ↑4
- [13] V.V. Williams, *Multiplying matrices in $O(n^{2.373})$ time* (2014). Online available at <http://theory.stanford.edu/~virgi/matrixmult-f.pdf>. ↑5